Утверждены Правлением
ООО РНКО «РИБ»
Протокол №6
от 09 июня 2017 г

УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ООО РНКО «РИБ»

Условия предоставления услуг дистанционного банковского обслуживания ООО РНКО «РИБ» (далее Условия обслуживания) – внутренний документ ООО РНКО «РИБ», определяющий условия оказания услуг дистанционного банковского обслуживания, описывающий правила информационной безопасности при использовании системы, процедуры доказательства подлинности электронного платежного документа, риски использования системы. Условия опубликованы на сайте www.ribank.ru.

ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

Если явно не оговорено иное, термины и определения, используемые в настоящем документе, имеют следующее значение:

Счета, Счет – банковские счета (банковский счет) в Российских рублях и/или в иностранной валюте, открытые (открытый) Клиенту в Банке в соответствии с действующим законодательством Российской Федерации и заключенными (заключенным) между Клиентом и Банком договорами (договором).

Договор (Договоры) банковского счета – заключенный (заключенные) между Банком и Клиентом договоры, на основании которых Банк открыл Клиенту Счет (Счета) и осуществляет расчетно-кассовое обслуживание Клиента.

Уполномоченное лицо Клиента – указанное в карточке с образцами подписей и оттиска печати (Клиента физическое лицо, имеющее право распоряжаться денежными средствами, находящимися на Счете (Счетах), с использованием электронной цифровой подписи.
Соглашение – Дополнительное соглашение к Договору банковского счета о принятии Клиента на обслуживание в Системе.

Система дистанционного банковского обслуживания (далее – Система) – корпоративная информационная система «BeSafe», представляющая собой совокупность программного, информационного и аппаратного обеспечения, включая программный комплекс, состоящий из средств формирования, обработки, хранения, передачи электронных документов и средств электронной цифровой подписи, реализующая электронный документооборот между Клиентом и Банком в соответствии с настоящим Договором.
Удостоверяющий центр – Закрытое акционерное общество «Центр Цифровых Сертификатов» (ИНН 5407187087; ОГРН 1025403189602) (http://www.besafe.ru), осуществляющее следующие функции:

- создает ключи электронных цифровых подписей и удостоверяет сертификаты ключей подписи и шифрования для персонального и корпоративного пользования;
- приостанавливает и возобновляет действие сертификатов ключей подписи (шифрования), а также аннулирует их;
- ведет реестр сертификатов ключей подписи (шифрования), обеспечивает его актуальность и возможность доступа к нему участников информационных систем;
- выдает сертификаты ключей подписи в электронной форме и (или) в форме документов на бумажных носителях с информацией об их действии;
- осуществляет проверку на уникальность идентификатора владельца сертификата ключа подписи (шифрования) в реестре сертификатов ключей подписи (шифрования);
- осуществление по обращениям пользователей сертификатов ключей подписей подтверждения подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.

Оператор Системы – Межбанковский процессинговый центр Faktura.ru (http://www.faktura.ru), являющийся участником Системы,

созданный Закрытым акционерным обществом «Биллинговый центр» (ИНН 5401152049; ОГРН 1025400512400) в целях информационного и технологического обслуживания Системы.

Банк – ООО РНКО «РИБ», осуществляющий все или часть функций Удостоверяющего центра на основании заключенного с ним соглашения.

Электронный документ (далее - ЭД) – документ, в котором информация представлена в электронно-цифровой форме.

Электронная цифровая подпись (далее - ЭЦП) – реквизит ЭД, предназначенный для защиты данного ЭД от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в ЭД.

Средства ЭЦП – программные средства, обеспечивающие реализацию хотя бы одной из следующих функций: создание ЭЦП в ЭД с использованием закрытого ключа ЭЦП, подтверждение подлинности ЭЦП в ЭД с использованием открытого ключа ЭЦП, создание закрытых и открытых ключей ЭЦП.

Закрытый ключ ЭЦП – уникальная последовательность символов, известная владельцу сертификата ключа ЭЦП и предназначенная для создания в ЭД ЭЦП с использованием Средств ЭЦП.

Открытый ключ ЭЦП – уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, доступная Сторонам и предназначенная для подтверждения подлинности ЭЦП в ЭД с использованием Средств ЭЦП.

Сертификат ключа ЭЦП – документ на бумажном носителе или ЭД с ЭЦП Банка, которые включают в себя открытый ключ ЭЦП и которые выдаются Банком Клиенту для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа ЭЦП.
Владелец сертификата ключа ЭЦП – уполномоченное Клиентом физическое лицо, наделенное правом распоряжения находящимися на Счете Клиента денежными средствами с использованием ЭЦП, на имя которого Банком зарегистрирован Сертификат ключа ЭЦП и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью Средств ЭЦП создавать свою ЭЦП в ЭД (подписывать ЭД).
Электронный документооборот – обмен ЭД между Сторонами в Системе в соответствии с настоящим Договором.

Электронное распоряжение на совершение переводов (далее – ЭПД) – ЭД, подписанный необходимым количеством ЭЦП представителей Клиента, уполномоченных распоряжаться находящимися на Счете Клиента денежными средствами с правом первой или второй подписи, и являющийся основанием для совершения операций по Счетам Клиента.

Электронный служебно-информационный документ (ЭСИД) – ЭД, не являющий платежным документом (выписки по счету, запросы, отчеты, информационный сообщения и т.п.).
Согласованный канал связи – сеть Интернет.

Подтверждение подлинности электронной цифровой подписи в электронном документе (проверка ЭЦП документа) –

положительный результат проверки соответствующими программными Средствами ЭЦП принадлежности ЭЦП в ЭД владельцу Сертификата ключа ЭЦП и отсутствия искажений в ЭД, подписанном данной ЭЦП.

Носитель ключевой информации – физический носитель информации определенной структуры, предназначенный для размещения на нем ключевой информации.

Автоматизированное рабочее место (АРМ) Клиента/Банка – аппаратно-программный комплекс, в состав которого входит программное обеспечение, предназначенное для:

- создания ЭД, подписания их ЭЦП, шифрования и передачи с АРМ Клиента на АРМ Банка и с АРМ Банка на АРМ Клиента;
- приёма и расшифровывания ЭД, проверки корректности ЭЦП, обработки информации из принятых ЭД;
- создания ключей ЭЦП и запросов на сертификаты открытых ключей ЭЦП;
- обработки и хранения сертификатов открытых ключей ЭЦП.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного ЭД.

Компрометация ключа ЭЦП – событие, в результате которого возможно несанкционированное использование неуполномоченными лицами закрытого ключа ЭЦП (в том числе несанкционированное списание или попытка списания денежных средств со счета Клиента). К таким событиям относятся, включая, но не ограничиваясь, следующие:

- утрата или порча Носителя ключевой информации;
- утрата носителя ключевой информации с последующим обнаружением;
- утрата ключей от сейфа (в том числе с последующим обнаружением) в момент нахождения в нем Носителя ключевой информации;
- временный доступ посторонних лиц к Носителям ключевой информации либо подозрение, что такой доступ имел место;
- нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа ЭЦП;
- случаи, когда нельзя достоверно установить, что произошло с носителями электронных ключей, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и достоверно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);
- иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа к носителям ключевой информации посторонних лиц.

Прочие термины и сокращения, используемые в настоящем документе, соответствуют законодательству Российской Федерации, нормативным актам Банка России, а также заключенным между Сторонами Договорам банковских счетов.

ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Дистанционное банковское обслуживание с использованием системы Клиент-Банк (Интернет-банкинг) (далее – Системы) предоставляется Клиентам Банка, с которыми заключен Договор банковского счета и (или) договор текущего валютного счета.

1.2. Настоящие Условия регламентируют порядок и условия предоставления услуги дистанционного банковского обслуживания Клиентов с использованием Системы.

1.3. Обмен электронными документами с Банком может осуществляться с компьютера Клиента с установленной операционной системой Windows 2000 и выше, программой Microsoft Internet Explorer v.5.5. и выше, настроенного для работы с Системой, при условии наличия у Клиента ключей электронной цифровой подписи (ЭЦП), необходимой для регистрации в Системе. Обмен электронными документами с Банком Клиент так же может осуществлять с использованием системы 1С: Предприятие, ни запуская при этом в Microsoft Internet Explorer, для этого необходим компьютер с установленной операционной системой не ниже Windows 2000 и 1С: Предприятие не ниже версии 8.1.

1.4. Безопасность использования Системы достигается за счет предоставления доступа Клиенту к возможностям Системы путем аутентификации пользователя с использованием ключа. Обмен документами между Банком и Клиентом основывается на том, что стороны признают использование средств криптографической защиты информации достаточным для обеспечения конфиденциальности, целостности и авторства электронных документов.

1.5. В качестве электронных носителей ключей ЭЦП могут использоваться съемные электронные носители (дискеты, флэш-карты, смарт-ключи). Использование жесткого диска компьютера для хранения ключей ЭЦП не рекомендуется.

1.6. На каждого сотрудника Клиента, уполномоченного работать с системой Клиент-Банк, изготавливается индивидуальный сертификат ключа ЭЦП.

1.7. Стороны признают, что получение Сторонами с использованием Системы электронных документов, подписанных ЭЦП, юридически тождественно получению аналогичных документов на бумажном носителе, с подписями уполномоченных лиц и печатью другой стороны, оформленных в соответствии с законодательством РФ и нормативными документами Банка России.

1.8. В соответствии с Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных» Клиент дает свое согласие ООО

РНКО «РИБ» (телефон (495) 232-34-34, адрес местонахождения: 119146, Москва, Фрунзенская наб., д. 24/1) на передачу всех персональных данных в ЗАО «Центр Финансовых Технологий» с целью исполнения Банком договорных обязательств перед клиентом. Согласие предоставляется с момента подписания Клиентом договора и действительно в течение пяти лет после исполнения договорных обязательств. Согласие может быть отозвано Клиентом в любой момент путем передачи Банку подписанного письменного заявления, если иное не предусмотрено законодательством РФ. Указанные Клиентом персональные данные предоставляются в целях информационного обмена с Банком, проведения операций в Системе, исполнения договорных обязательств, а также разработки Банком новых продуктов и услуги информирования Клиента об этих продуктах и услугах.

1.9. Вся документация необходимая Клиенту для работы с системой Клиент-Банк размещена на сайте Банка (www.ribank.ru).

1.10. При изменении условий оказания услуг, Банком вводится в действие новая редакции Условий.

1.11. Банком установлено следующее операционное время для перевода денежных средств на основании электронных платежных документов, поступивших в Банк и прошедших процедуру приема к исполнению распоряжений Клиентов на перевод денежных средств (контроль) в рабочие дни, установленные на территории Российской Федерации (время московское):

- в валюте Российской Федерации – с 09 часов 00 минут до 17 часов 45 минут;
- в иностранной валюте – с 09 часов 00 минут до 12 часов 00 минут;

-по выполнению поручений Клиента по операциям покупки – продажи иностранной валюты – с 09 часов 00 минут до 12 часов 00 минут.

1.12. Электронные платежные документы в валюте РФ, поступившие в Банк с видом платежа «Срочно», в течении операционного времени, принимаются к исполнению и проводятся через банковскую электронную систему переводов (БЭСП) в тот же день не позднее одного часа с момента поступления в Банк.

1.13. При недостаточности денежных средств на банковском счете Клиента распоряжения не принимаются Банком к исполнению и возвращаются не позднее рабочего дня, следующего за днем поступления распоряжения, за исключением:

- распоряжений о переводе денежных средств в бюджет Российской Федерации,

- распоряжений этой же и предыдущей очередности списания денежных средств со счета Клиента. Банк направляет Клиенту посредством Системы уведомление о неисполнении/ возврате распоряжения.

1.14. Принятые к исполнению распоряжения о переводе денежных средств в бюджет Российской Федерации, распоряжения этой же и предыдущей очередности списания денежных средств со счета Клиента, помещаются Банком в очередь не исполненных в срок распоряжений для дальнейшего контроля достаточности денежных средств и исполнения в срок и в порядке очередности списания денежных средств со счета Клиента, которые установлены Федеральным законом.

1.15. При наличии приостановлений в соответствии с Федеральным законом операций по счету Клиента распоряжения, находящиеся в очереди не исполненных в срок распоряжений, помещаются в очередь распоряжений, ожидающих разрешения на проведение операций. При отмене приостановления операций по счету Клиента указанные распоряжения подлежат исполнению.

1.6. Срок исполнения распоряжений Клиента, кроме поступивших с видом «Срочно» устанавливается договором банковского счета и/или Тарифами Банка.

ПОРЯДОК ЗАКЛЮЧЕНИЯ СОГЛАШЕНИЯ О ДИСТАНЦИОННОМ БАНКОВСКОМ ОБСЛУЖИВАНИИ

2.1. Информация об услуге дистанционного банковского обслуживания с использованием системы Клиент-Банк и формы документов размещены на сайте Банка (www.ribank.ru).

2.2. Заключение соглашения на дистанционное банковское обслуживание состоит из следующих этапов:

2.2.1. Изучение Клиентом Условий обслуживания размещенных на сайте Банка (www. ribank.ru);

2.2.2. Подготовка и передача в Банк пакета документов необходимых для заключения Соглашения;

2.2.2. Выбор Клиентом типа ключевого носителя;

2.2.3. Генерация Банком ключей ЭЦП;

2.2.4. Регистрация ключа ЭЦП Банком в Системе;

2.3. Типы ключевых носителей, на которых будут храниться ключи ЭЦП: дискета, флэш-карта, смарт-ключ и т.п.

От выбора типа ключевого носителя зависит степень безопасности использования Системы и процедура регистрации сеансов подключения к Системе в процессе работы:

Дискета, флэш-карта – в связи с наличием в сети Интернет специально разработанных вирусных программ, похищающих с компьютеров пользователей файлы с ключами ЭЦП систем дистанционного банковского обслуживания, степень безопасности использования системы зависит от эффективности антивирусной защиты компьютера Клиента. С целью повышения безопасности при использовании указанных выше типов ключевых носителей, после каждой авторизации клиента в Системе (ввода логина и основного пароля), предусмотрена необходимость ввода дополнительного одноразового пароля, который Клиент получает сразу после авторизации в Системе в виде SMS сообщения на номер мобильного телефона, указанный им при заключении Соглашения.

Смарт-ключ – специальное электронное устройство с USB разъемом, содержащее встроенный процессор, выполняющее операцию подписания электронных документов электронной цифровой подписью способом, исключающим возможность хищения ключей ЭЦП. При хранении ключей ЭЦП на смарт-ключе, использование одноразовых паролей носит рекомендательный характер.

2.4. Банк, являясь Агентом Удостоверяющего центра, на основании полученного от Клиента Заявления на выдачу сертификата ключа и Анкеты, инициирует выпуск сертификата ключа Клиента.

2.5. Удостоверяющий центр выпускает электронный сертификат ключа.

2.6. Банк записывает сертификат на ключевой носитель, получает Акт приема-передачи, распечатывает Акт приема-передачи в двух экземплярах, подписывает и ставит печать. Один экземпляр Акта передается Клиенту.

2.7. На каждого сотрудника Клиента, уполномоченного работать в Системе, изготавливается индивидуальный ключ ЭЦП.

2.8. В случае если уполномоченный сотрудник является представителем нескольких Клиентов и существует необходимость работать в Системе с использованием одного ранее выпущенного ключа (ключ должен быть выпущен на физическое лицо).

2.9. С целью подключения к системе Клиент передает в Банк следующие документы, оформленные с его стороны и достаточные для его подключения к Системе:

Заявление на подключение к Системе – 1 экз.; Анкету уполномоченного сотрудника – 1 экз. на каждого сотрудника;

Дополнительное соглашение к договору банковского счета с приложениями – 2 экз.;

2.10. Соглашение считается заключенным с момента его подписания Банком.

2.11. Обслуживание Клиента с использованием Системы начинается не позднее следующего банковского дня после подписания Банком Акта приема передачи сертификата (ключа ЭЦП).

2.12. В случае просрочки Клиентом оплаты комиссии за регистрацию в Системе и выдачу ключа ЭЦП на срок более 30 (Тридцать) календарных дней Банк вправе приостановить обслуживание Клиента на срок до момента погашения Клиентом задолженности.
2.13. В случае непогашения Клиентом задолженности в течении 3 (Три) месяцев, Соглашение расторгается.

ПОРЯДОК ЭКСПЛУАТАЦИИ СИСТЕМЫ

3.1. Если не оговорено особо, в рамках Соглашения Клиент может: 3.1.1. работать со следующими документами:

- выписка по счету;
- платежное поручение;
- перевод валюты;
- покупка, продажа, конверсия валюты;
- уведомление о получении валютной выручки;
- подтверждение остатка на счете клиента;
- документы свободного формата;

- документы валютного контроля.

3.1.2. получать SMS уведомления (Системой может взиматься дополнительная плата): - о входе в Систему; - одноразовые пароли;

- содержащие информацию о снятии/поступлении на расчетный счет.

3.1.3. получать E-mail уведомления:

- о входе в систему;
- об исполнении документов, отправленных в Банк;
- о поступлении из Банка выписки или промежуточной информации об операциях по счету;
- о поступлении валютной выручки;
- о поступлении документов свободного формата;
- о замене Банком ранее присланной выписки по счету;
- о поступлении новых почтовых сообщений;
- о поступлении из Банка запроса на подтверждение остатка;
- об увеличении остатка средств на счете;
- об уменьшении остатка средств на счете;
- об остатке средств на счете в указанное время (ежедневно).

Осуществлять обмен электронными документами с Банком непосредственно из 1С: Предприятие, не запуская Microsoft Internet Explorer.

3.2. Отправка и прием электронных документов должны осуществляться только владельцем ключа ЭЦП.

3.3. Для предоставления доступа к счетам новым сотрудникам, Клиент в отношении каждого сотрудника предоставляет в Банк Анкету в одном экземпляре на бумажном носителе.

3.4. Для изменения прав доступа владельцев ключей ЭЦП к счетам Клиента открытым в Банке, Клиент предоставляет в Банк Заявление о замене ключа ЭЦП в одном экземпляре на бумажном носителе.

3.5. Для подключения к Системе новых счетов, открытых в Банке, Клиент предоставляет в Банк Заявление на подключение\отключение счетов к системе Клиент-Банк в одном экземпляре на бумажном носителе.

3.6. Электронный документ считается принятым Банком к исполнению, если его статус изменен с «Доставлен в банк» на иной.

3.7. Клиент вправе отозвать отправленный электронный документ, если Банком не начата его обработка (статус документа, отправленного в Банк изменен на «Исполнен»). Отзыв переданного в Банк платежного документа может быть произведен Клиентом только после устного распоряжения (по телефону) с последующей обязательной отправкой Банку отзыва по Системе («Прочие документы») с полным указанием реквизитов отзываемого документа. После исполнения Банком распоряжения Клиента об отзыве платежного документа, документ приобретает статус «Возвращен» с указанием причины возврата.

3.8. Электронные документы вместе с их ЭЦП должны храниться Сторонами в течение времени, установленного для аналогичных документов на бумажном носителе, если иное не предусмотрено действующим законодательством РФ.

ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

4.1. Электронный документооборот между Клиентом и Банком может включать в себя следующие этапы:

4.1.1. Формирование электронного документа;

4.1.2. Отправку и доставку электронного документа;

4.1.3. Проверку электронного документа;

4.1.4. Подтверждение получения электронного документа;

4.1.5. Отзыв электронного документа;

4.1.6. Хранение электронных документов (ведение архивов).

4.2. Система позволяет использовать несколько вариантов формирования электронных документов:

4.2.1. Подготовка электронных документов в режиме on-line, путем заполнения типовых экранных форм документов, реализованных в Системе. Этот вариант подходит для Клиентов, работающих с небольшим количеством документов в день и использующих типовые формы документов, реализованных в Системе.

4.2.2. Подготовка документов, в том числе платежных, в off-line с использованием специализированного программного обеспечения (приложения Microsoft, бухгалтерские программы и прочее) с последующим импортом данных в Систему.

4.2.3. Для некоторых бухгалтерских программ (например, 1С - бухгалтерия) существуют интегрированные в Систему модули сопряжения, позволяющие экспортировать и импортировать документы в Систему.

4.3. Электронные документы могут отправляться Клиентом в Банк только после их подписания ЭЦП. В случае неверного оформления документа, отправленного Клиентом в Банк или в случае подписания документа неверным ЭЦП, документ к обработке не принимается, о чем Клиент извещается средствами Системы с указанием причины отказа.

4.4. Система позволяет Клиенту отслеживать статус каждого отправленного в Банк документа, который может иметь следующие состояния:

4.4.1. Подготовлен – документ подготовлен, но не отправлен в Банк. На данном этапе электронный документ можно исправить или удалить;

4.4.2. Подписан – такой статус возникает, если под документом должно быть несколько подписей (первая и/или вторая и/или подтверждающая);

4.4.3. Отправлен в банк – документ отправлен в Банк, но еще не получен Банком;

4.4.4. Принят банком – документ получен Банком, прошел проверку на подлинность подписи, но еще не обработан;

4.4.5. Исполнен – документ исполнен Банком;

4.4.6. Возвращен – документ возвращен Клиенту с указанием причины.

4.5. Клиент и Банк самостоятельно ведут архив документов, отправленных\полученных с использованием Системы, обеспечивая целостность помещенных в них документов. Подписанные ЭЦП документы, помещенные в архив, должны храниться вместе с необходимой для подтверждения подписи ключевой информацией.

4.6. В Системе предусмотрена возможность информирования Клиентов о всех входах в Систему и о получении Банком платежных документов от имени Клиента, путем отправки на номер мобильного телефона, указанный им при заключении Договора,

соответствующих SMS-сообщений. Активация услуги информирования может быть выполнена и после заключения Соглашения, путем подачи соответствующего заявления.

4.7. В случае изменения номеров контактных телефонов или адресов e-mail, используемых для информирования Клиентов о получении Банком платежных документов от имени Клиента и о всех входах в Систему, Клиенты обязаны немедленно направить в Банк Заявление об изменении контактных данных.

СЕРТИФИКАТЫ КЛЮЧЕЙ ЭЦП И КЛЮЧИ ЭЦП

5.1. Изготовление Сертификатов ключей ЭЦП осуществляется на основании Заявления Клиента, поданного им Банку. Заявление формируется в соответствии с типовой формой, разработанной Банком и подписывается собственноручно Клиентом или его уполномоченным лицом. Содержащиеся в Заявлении сведения подтверждаются предъявлением соответствующих документов (для физических лиц – паспорт, для представителей юридических лиц – паспорт, а также письменный документ, заверенный подписью руководителя и печатью организации, подтверждающий право представителя действовать от имени данной организации).

5.2. Сертификат ключа ЭЦП содержит следующие данные:

5.2.1. Уникальный идентификатор владельца сертификата ключа (ФИО или псевдоним, или учетный идентификатор владельца сертификата ключа подписи, дополнительные сведения);

5.2.2. Открытый ключ;

5.2.3. Идентификатор сертификата ключа Удостоверяющего центра, создавшего сертификат ключа;

5.2.4. Уникальный регистрационный номер сертификата ключа, присвоенный Удостоверяющим центром;

5.2.5. Дату начала и окончания срока действия сертификата ключа;

5.2.6. Идентификатор Удостоверяющего центра, выдавшего сертификат ключа;

5.2.7. Подпись Удостоверяющим центром данных Сертификата ключа.

5.3. Клиент обязан обеспечить конфиденциальность и безопасность закрытых ключей ЭЦП используемых в Системе.

5.4. В силу особенностей формирования закрытых ключей ЭЦП Удостоверяющим центром, Банк не имеет к ним доступа, в случае выявления фактов компрометации ключей, претензии к Банку не могут быть предъявлены.

5.5. С целью обеспечения конфиденциальности и безопасности закрытых ключей ЭЦП, используемых в Системе, Клиент должен соблюдать следующие меры предосторожности:

5.5.1. использовать и своевременно обновлять на компьютере, с которого осуществляется работа с Системой, антивирусное программное обеспечение;

5.5.2. применять технические и организационные меры, исключающие возможность доступа посторонних лиц к ключевым носителям;

5.5.3. при наличии малейших подозрений о компрометации ключей, уведомлять об этом Банк и инициировать блокирование ключей до выяснения обстоятельств и/или выполнить мероприятия по смене ключей ЭЦП.

5.6. Банк настоятельно рекомендует не использовать в качестве ключевого носителя жесткий диск компьютера, так же рекомендует не использовать отчуждаемые носители (дискеты, флэш-карты т.п.) и настоятельно рекомендует использовать смарт-ключи.

СМЕНА СЕРТИФИКАТА КЛЮЧА ЭЦП И КЛЮЧЕЙ ЭЦП. ОБЩИЕ ПОЛОЖЕНИЯ

6.1. При изменении данных, идентифицирующих Владельца сертификата ключа ЭЦП, содержащихся в документах, предоставленных при выдаче Сертификата ключа ЭЦП, смене ключей ЭЦП, в случаях Компрометации ключей ЭЦП, Владельцу сертификата ключа ЭЦП надлежит получить новый Сертификат ключа ЭЦП в порядке, предусмотренном настоящим разделом. Все риски, связанные с невозможностью использования Сертификата ключа ЭЦП в связи с изменением данных, идентифицирующих Владельца сертификата ключа ЭЦП, несет Владелец сертификата ключа ЭЦП.

6.2. Сертификаты ключей ЭЦП, выдаваемые в Системе, действительны в течение одного года, после чего они должны быть обновлены, т.е. должны быть сгенерированы новые ключи ЭЦП и изготовлены новые Сертификаты ключей ЭЦП.

6.3. Если срок действия Сертификата ключа ЭЦП еще не истек, Клиент может обновить Сертификат ключа ЭЦП, передав в Банк Анкету и носитель ключевой информации, после чего Банк продлит срок действия закрытого ключа, подготовит Акт и передаст Клиенту.

6.4. Если срок действия Сертификата ключа ЭЦП не истек Клиент праве самостоятельно произвести продление срока действия Сертификата ЭЦП используя пункт меню «Обновление Сертификата ключа ЭЦП» в Личном кабинете. В этом случае Акт, подписанный ЭПЦ Банка придет на электронную почту Клиента. Клиент подпишет Акт своим ЭЦП.

6.5. Если срок действия Сертификата ключа ЭЦП истек, Клиенту необходимо передать в Банк Анкету и носитель ключевой информации, при этом Банком будут выполнены действия как при регистрации нового сотрудника.

6.56. Банк вправе отказать в выдаче Клиенту нового Сертификата ключа ЭЦП, с указанием причины отказа.

6.7. Смена Сертификата ключа ЭЦП, смена ключей ЭЦП в связи с Компрометация ключей ЭЦП может произойти в следующих случаях:

6.6.1. увольнение сотрудников, имевших доступ к ключевым носителям, если ЭЦП было выпущено, но на юридическое лицо;

6.6.2. неисправность ключевого носителя;

6.6.3. ключ стал известен третьим лицам.

6.8. В случае компрометации рабочих ключей ЭЦП, Клиент обязан в кратчайшие сроки уведомить Банк о факте компрометации. Для этого Клиент должен не позднее следующего рабочего дня предоставить в Банк Заявления о компрометации ключа ЭЦП на бумажном носителе в двух экземплярах, заверенных подписью и печатью Клиента, либо сканирует его, подписывает своей ЭЦП и направляет посредством Системы. Дата и время получения

заявления о компрометации фиксируется Администратором Системы по отметке времени получения Заявления. Один экземпляр Заявления, полученного на бумажном носителе, с отметкой времени возвращается Клиенту, другой - остается в Банке для использования его в дальнейшей работе.

Если Клиент не может оперативно приехать в офис Банка и подать заявление, Клиент вправе направить на электронный адрес Банка скан-копию Заявления о компрометации ключа.

Банк снимает в системе права на использование данного счета. После того, как Клиент принес в Банк оригинал Заявления о компрометации ключа, Банк инициирует процедуру компрометации.

6.9. По истечении не более чем 2 (двух) часов со времени получения Банком уведомления о компрометации ключа ЭЦП в рабочие дни, или не более чем 2 (двух) часов с начала первого рабочего дня для случая, когда уведомление о компрометации ключа ЭЦП было получено в электронном виде в нерабочие дни, все документы, полученные по Системе с использованием скомпрометированных ключей, считаются недействительными, не принимаются Банком в обработку и возвращаются Клиенту с указанием причины возврата.

6.10. Банк не несет ответственности за возможный ущерб, вызванный компрометацией ключа ЭЦП Клиента, в течение 2 (двух) часов с момента получения Банком уведомления о компрометации ключа ЭЦП в рабочие дни, или 2 (двух) часов с начала первого рабочего дня, если уведомление о компрометации ключа ЭЦП было получено в электронном виде в нерабочие дни.

6.11. После передачи в Банк Заявления о компрометации ключа ЭЦП, для возобновления работы уполномоченного лица Клиента в Системе, Клиенту необходимо выполнить действия, как при регистрации нового сотрудника.

6.12. Новый ключ уполномоченному сотруднику Клиента, в отношении ключа ЭЦП которого в Банк поступило уведомление о компрометации ключа ЭЦП, может быть выдан только после получения Банком Заявления о компрометации ключа ЭЦП.

ПОРЯДОК ИЗГОТОВЛЕНИЯ (ПЕРЕИЗГОТОВЛЕНИЯ) СЕРТИФИКАТОВ КЛЮЧА ЭЦП И КЛЮЧЕЙ ЭЦП

7.1. Банк изготавливает Сертификат ключа ЭЦП, а также ключи ЭЦП, руководствуясь следующими правилами:

7.1.1. Получив Заявление Клиента в соответствии с п. 5.1, Банк формирует запрос на создание Сертификата ключа ЭЦП. Запрос формируется в виде ЭД, подписанного ЭЦП Банка и направляется в Удостоверяющий центр с использованием программно-аппаратных средств Банка, подключенных через каналы связи к программно-техническим средствам Удостоверяющего центра. Запрос содержит Закрытый ключ ЭЦП, а также Уникальный идентификатор владельца сертификата ключа, сформированный на основе проверенных Банком данных Клиента.

7.1.2. Создание Сертификатов ключа ЭЦП для Банка/Клиентов осуществляется Удостоверяющим центром в течение 3 (Трех) рабочих дней с момента получения от Банка электронного запроса. Передача Удостоверяющим центром или уполномоченными им лицами Банку Носителей ключевой информации, содержащих Ключ ЭЦП и Сертификат ключа ЭЦП, созданных Удостоверяющим центром без получения Заявления от Клиента, осуществляется в порядке и на условиях, определяемых Удостоверяющим центром и Банком дополнительно.

7.1.3. При изготовлении Сертификатов ключа ЭЦП всегда проверяется уникальность Идентификаторов владельцев сертификатов ключа, принадлежащих разным Владельцам сертификатов ключа, и Открытых ключей ЭЦП в реестре и архиве Удостоверяющего центра. Программно-аппаратные средства Удостоверяющего центра исключают возможность изготовления одинаковых Сертификатов ключа ЭЦП. При изготовлении Носителей ключевой информации, Удостоверяющий центр самостоятельно формирует уникальный Идентификатор владельца сертификата и присваивает его созданному Сертификату ключа ЭЦП.

7.1.4.Удостоверяющий центр предоставляет Банку созданные по Заявлению/запросу Банка Сертификаты ключа ЭЦП для Банка/Клиентов в форме ЭД.

7.1.5. Банк при выдаче Криптографических ключей Клиента распечатывает на бумажном носителе Акт приема-передачи Сертификата ключа ЭЦП Клиента в двух экземплярах и обеспечивает проставление в них собственноручной подписи Клиента или уполномоченного лица Клиента. Второй экземпляр Акта приема-передачи на бумажном носителе хранится у Банка. По требованию Удостоверяющего центра Банк обязан направить в Удостоверяющий центр заверенную копию Акта. Направление заверенной копии осуществляется Банком за свой счет в течение не более 5 (Пяти) рабочих дней с даты получения соответствующего требования от Удостоверяющего центра. В случае не направления вышеуказанного Акта в предусмотренный срок, Удостоверяющий центр вправе приостановить деятельность такого Банка по формированию запросов на создание Сертификатов ключа ЭЦП и их выдачи Клиентам, письменно уведомив об этом Банк.

7.2. Клиент, уже являющийся Владельцем Сертификата ключа ЭЦП, изготавливает Сертификат ключа ЭЦП, посредством удаленного обращения на страницу сервера Удостоверяющего центра, предназначенную для удаленной выдачи Сертификатов ключа ЭЦП, руководствуясь следующими правилами:

7.2.1. Банк обращается на сервер Удостоверяющего центра и подтверждает выдачу нового Сертификата ключа ЭЦП Клиента.

7.2.2. Удостоверяющий центр изготавливает новый Сертификат ключа ЭЦП по запросу Клиента. Класс нового Сертификата ключа ЭЦП совпадает с Классом действующего Сертификата ключа ЭЦП Клиента.

7.2.3. Банк обращается на сервер Удостоверяющего центра и получает Акт приема-передачи нового Сертификата ключа ЭЦП Клиента.

7.2.4. Банк заверяет Акт приема-передачи нового Сертификата ключа ЭЦП Клиента Электронной подписью и передает его Удостоверяющему центру, подтверждая тем самым выдачу нового Сертификата ключа ЭЦП Клиенту.

7.2.5. Банк или Удостоверяющий центр сообщает Клиенту адрес выдачи нового Сертификата ключа ЭЦП.

7.2.6. Клиент обращается по указанному адресу, получает заверенный Банком Акт приема-передачи нового Сертификата ключа ЭЦП.

7.2.7. Клиент заверяет действующей ЭП Акт приема-передачи нового Сертификата и передает Акт в УЦ.

7.2.8. Клиент получает новый Сертификат ключа ЭЦП.

7.2.9. Сертификат ключа ЭЦП помещается в реестр Сертификатов, который ведет Удостоверяющий центр.

7.2.10. Так как Акт приема-передачи формируется в электронном виде и сохраняется Удостоверяющим центром, Банк может в этом случае Акт не хранить.

7.2.11 Банк может отказаться от подтверждения выдачи нового Сертификата ключа ЭЦП Клиента, при этом Банк или Удостоверяющий центр направляет Клиенту сообщение об отказе.

7.3. Правила, указанные в п. 7.2. (включая соответствующие подпункты 7.2.1. - 7.2.11.), применяются, только в случаях, когда:

- Клиент, уже являющийся Владельцем сертификата ключа ЭЦП Удостоверяющего центра, срок действия которого не истек, формирует новую пару Открытого ключа ЭЦП и Закрытого ключа ЭЦП, а также запрос на новый Сертификат ключа ЭЦП;
- Клиент подписывает запрос на новый Сертификат ключа ЭЦП действующим Закрытым ключом ЭЦП. Идентификаторы владельца сертификата нового и действующего Сертификата ключа ЭЦП должны совпадать;
- Клиент передает заверенный действующим Закрытым ключом ЭЦП запрос на новый Сертификат ключа ЭЦП серверу Удостоверяющего центра. Запрос равнозначен Заявлению Клиента на выдачу Сертификата ключа ЭЦП, заверенному собственноручной подписью Клиента или уполномоченного лица Клиента.

ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ ВОЗНИКАЮЩИХ В ХОДЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

8.1. Споры, возникающие в ходе электронного документооборота между Клиентом и Банком следующего характера:

8.1.1. оспаривание факта формирования Клиентом или Банком электронного документа;

8.1.2. оспаривание времени и даты отправки\доставки электронного документа одной из сторон;

8.1.3. заявление одной из сторон об искажении электронного документа;

8.1.4. другие споры требующие проверки подлинности ЭЦП, передаются на рассмотрение Комиссии, формируемой на основании письменного заявления Клиента или Банка другой Стороне.

8.2. В состав Комиссии входят в равных количествах представители Сторон.

8.3. Основанием для проведения разбора конфликтных ситуаций является письменное заявление от одной из Сторон направленное в адрес другой Стороны, о возникновении конфликтной ситуации.

8.4. Целью проведения разбора конфликтной ситуации является подтверждение или не подтверждение подлинности ЭЦП под документом, являющимся предметом спора Сторон.

8.5. Рассмотрение конфликтных ситуаций выполняется специально создаваемой Комиссией, состоящей из представителей Банка и представителей Клиента, при необходимости могут быть дополнительно привлечены специалисты Удостоверяющего центра и / или Оператора Системы.

8.6. Все виды конфликтных ситуаций, описываемых в данном документе, связаны с доказательством целостности, подлинности электронных документов, факте, либо времени его получения или отправки.

8.7. Электронный документ считается подлинным, если он был одной Стороной надлежащим образом сформирован, подписан и отправлен, а другой Стороной - получен, проверен и принят. Свидетельством факта получения документа является наличие уведомления о получении электронного документа, сформированного и отправленного системой Клиент-Банк. Свидетельством времени получения, отправки или факта подписания электронного документа является метка времени в электронном документе, содержащая время системы Клиент-Банк и связанная с использованием криптографических протоколов с электронным документом, для которого требуется освидетельствование.

8.8. Комиссия по разбору конфликтных ситуаций создается по письменному заявлению одной из участвующих в конфликте Сторон не позднее 5 (Пять) рабочих дней с момента получения Стороной письменного заявления для разрешения конфликтов, предметом которых являются:

8.8.1. отказ подписывающей Стороны от факта подписи электронного документа;

8.8.2. отказ подписывающей Стороны от содержания электронного документа;

8.8.3. отказ Стороны-получателя электронного документа от факта получения электронного документа;

8.8.4. отказ Стороны-отправителя электронного документа от факта отправки электронного документа;

8.8.5. отказ Стороны-получателя электронного документа от времени получения электронного документа;

8.8.6. отказ Стороны-отправителя электронного документа от времени отправки электронного документа.

8.9. Комиссия созывается Банком. В состав Комиссии входят равное количество представителей Сторон. Рекомендуемым числом членов Комиссии с каждой стороны является по 3 человека: 2 человека представляют руководство и финансовое подразделение, 1 человек – службу информационных технологий. Комиссия осуществляет свою работу на территории Банка.

8.10. До подачи заявления, заявитель должен убедиться, что причиной возникновения конфликта не является нарушение целостности программного обеспечения, произошедшего в результате сбоев аппаратуры, действия компьютерных вирусов или троянских программ.

8.11. Для участия в работе Комиссии, представители Сторон должны иметь с собой Акт приема-передачи сертификата ключа и ключевой носитель, на котором хранится закрытый ключ ЭЦП.

8.12. Для работы Комиссии Банк предоставляет необходимое оборудование и программное обеспечение.

8.13. Перед проведением разбора конфликтной ситуации, Комиссия проверяет ЭЦП сертификатов ключей Сторон, для чего из архива сертификатов получаются эталонные копии сертификатов, и Комиссия сверяет их с сертификатами представленными сторонами.

8.14. Проверка подлинности документа, подписанного закрытым ключом ЭЦП и достоверность идентификации Сертификата, выполняются с использованием Эталонного Модуля Проверки подписи документа, хранящегося у Удостоверяющего центра. Результатом работы Эталонного Модуля Проверки является:

8.14.1. установление факта создания спорного документа с использованием Системы;

8.14.2. установление факта подписи спорного документа в соответствии с технологией Системы;

8.14.3. установление факта целостности спорного документа.

8.15. Подтверждение подлинности ЭЦП под спорным документом означает, что документ действительно подписан владельцем закрытого (секретного) ключа ЭЦП и электронный документ юридически тождественен аналогичному документу на бумажном носителе заверенному подписью уполномоченных лиц и печатью Стороны-отправителя документа.

8.16. Не подтверждение подлинности ЭЦП под спорным документом означает, что электронный документ не имеет юридической силы.

8.17. После проведения разбора конфликтной ситуации, Комиссия составляет протокол проверки. Решение Комиссии в виде Акта, отражающего результаты проверки, оформляются в письменном виде и подписывается собственноручно членами Комиссии. Решение Комиссии является окончательным и пересмотру не подлежит. Действия, вытекающие из решения, являются обязательными для обеих Сторон конфликта.

8.18. Возмещение пострадавшей Стороне принесенного ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА КЛИЕНТОВ

9.1. Клиент вправе обратиться для получения необходимых консультаций, технической и методической помощи в работе с Системой по телефонам, указанным на сайте Банка (www.ribank.ru) в рабочее время. Дистанционные консультации по телефону оказываются бесплатно.

9.2. Клиент вправе вызвать сотрудника Банка в свой офис для настройки Системы и обучения принципам работы в Системе. Данные услуги оказываются Банком при наличии у Банка возможности и оплачиваются отдельно.